EXPRESS MAIL MAILING LABEL
No. EM401140420US
Utility Patent Application
CTX-052
(1545/90)

STRONG MUTUAL AUTHENTICATION OF DEVICES

RELATED APPLICATION

The application entitled "Secure Exchange of an Authentication Token" designated by attorney docket number CTX051 filed concurrently with the present application and owned by the assignee of the present application is herein incorporated by reference.

FIELD OF THE INVENTION

The invention relates in general to secure communication systems and more specifically systems enabling mutual authentication of devices.

BACKGROUND OF THE INVENTION

When dealing with electronic commerce, security of information on a network is a problem faced by individuals and companies alike. For example, the security today between a user's computer and server computer in an electronic transaction does not preclude the user from fraudulently quoting another user's identification information, such

as a user's password, credit card number, or social security number. Likewise, a server could similarly be fraudulently represented on the user's computer by someone to obtain the unsuspecting user's information. Therefore, in business transactions occurring over the internet today, full electronic commerce necessitates stronger authentication between the user's computer and the server computer.

For stronger authentication of both users and server computers, encryption and decryption may be used for the transmission of messages. The major barrier to mutual authentication of a user's computer communicating with a server computer is the inability of personal computers to provide tamperproof and confidential storage for these keys, which are vital for security of transmitted information. Smart cards, or credit-card sized devices that have user information embedded within the card, have recently addressed this issue. However, the smart cards are only as useful as the number of smart card readers available, which currently have not been widely adopted.

Therefore, it is desirable to produce an equivalent but unrestricted method to allow strong mutual authentication between devices.

SUMMARY OF THE INVENTION

The invention relates to a method for enabling strong mutual authentication between two computers or devices in a communication system. In one embodiment, the communication system includes a first computer in communication with a second computer. A user attempting to gain access to the first computer transmits login information via a second computer over a first communication channel to the first computer. The first computer transmits a first message, which in one embodiment includes a first key encrypted by a second key, to the second computer over the first communication channel. The second computer does not have access to the second key, and so cannot decrypt the first message to obtain the first key.

The first computer then transmits a second message to a third device associated with the user over a second communication channel. The second message includes the second key that the second computer needs to decrypt the first message transmitted by the first computer. In one embodiment the second key included in the second message is encrypted with a public key associated with the user. The second message in one embodiment also

includes the user's login information. The third device, in one embodiment, uses the user's login information to obtain the private key associated with the user, which the third device uses to obtain the second key.

The third device transmits the second key in a third message to the second computer over a third communication channel. The second computer uses the thereby attained second key to decrypt the first message and obtain the first key.

Once the second computer obtains the first key, in one embodiment the second computer switches the role of the keys from the first message by encrypting the second key with the first key into a fourth message. The second computer transmits the fourth message to the server over the first communication channel, and the first computer subsequently decrypts the fourth message using its first key. If the second key received from the fourth message is the same as the second key used in the first message, then the second computer is authenticated to the first computer.

DESCRIPTION OF THE DRAWINGS

The aspects of the invention presented above and many of the accompanying advantages of the present invention will become better understood by referring to the

included drawings, which show a system according to the preferred embodiment of the invention and in which:

FIG. 1 is a diagram of the steps and protocol followed in an embodiment of the communications system of this invention to mutually authenticate the user and components of the communications system.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

In brief overview, the present invention relates to a method for enabling strong mutual authentication between a first computer or device and a second computer or device which are in communication. Referring to FIG. 1, the first computer 30, also referred to as a server (S), communicates with the second computer 10, also referred to as a client (C), over a communication channel 15. The client (C) 10 begins the authentication routine by transmitting (step 105) information about a user (U) who is attempting to gain access to the server (S) 30 by way of the client (C) 10. The server (S) 30 transmits (step 125) a first message ({k}r) 63, which, in one embodiment, includes a first key (k) encrypted with a second key (r), to the client (C) 10. In one embodiment the first key (k) is a session key and is used only to authenticate communications between the server (S) 30 and the client (C) 10.

Authentication of the client (C) 10 to the server (S) 30 will occur when the client (C) 10 transmits a message back to the server (S) 30 which includes the second key (k). In one embodiment the message is the second key (r) encrypted with the first key (k). In order for the client (C) 10 to send the second key (r) back to the server (S) 30 or to send the second key (r) encrypted with the first key (k) back to the server (S) 30, it must first decrypt the first message ({k}r) 63 to obtain the first key (k). However, to decrypt the first message ({k}r) 63 the client 10 needs the second key (r), which it does not have access to in its memory.

To provide the client (C) 10 with the second key (r), the server (S) 30 begins by transmitting (step 135) a second message 35 to a third device, or verifier 50 associated with the user (U). In one embodiment the verifier 50 is a telephone associated with the user (U). In one embodiment, the second message 35 includes an encrypted portion, which includes the second key (r) encrypted with a third key (u+) (that is: ({r}u+)), and encryption key information. In one embodiment, the encryption key information is the user's information, such as the user's username and is also designated by (U). In one embodiment, the second key (r) encrypted with the third key (u+) and the encryption key information (U) are all encrypted with a fourth key (s-) (that is: ({U,{r}u+}s-)). In one embodiment the third key

(u+) is the user's public key and the fourth key (s-) is the server's private key. The second message 35 also includes a non-encrypted portion, which indicates what key is to be used to decrypt the second message 35. In one embodiment the non-encrypted portion includes the designation (S) of the server (S) 30. Thus, the second message 35 may be written as (S,{U,{r}u+}s-).

When the verifier 50 receives the second message 35, it is able to read the non-encrypted portion and extract the server designation (S) to determine what key is to be used in decrypting the second message 35. By reading the server designation (S), the verifier 50 knows that the key (s-) was used to encrypt the encrypted portion of the second message 35 and can thereby decrypt it (step 140). In the embodiment in which (s-) is the server's private key, the designator (S) indicates to the verifier 50 that the server's public key (s+) should be used to decrypt the message. From this decryption the verifier 50 is able to obtain encryption key information about the user (U) and from this information determine that the third key (u+) was used to encrypt the second key (r). In the embodiment in which the user's public key (u+) was used to encrypt the message, the designator (U) instructs the verifier 50 to use the user's private key (u-) which in one embodiment is stored on the verifier 50, to decrypt the message. From this information the verifier 50 can determine (r).

The verifier 50 subsequently transmits (step 170) the second key (r) in the third message 60 to the client (C) 10 over a communication channel 55. In one embodiment the communication channel 55 is the user (U), who simply reads the second key (r) from the display on the verifier 50 and enters it into the client (C) 10. With the newly received second key (r), the client (C) 10 can decrypt (step 175) the first message ({k}r) 63 received from the server (S) 30 to obtain the first key (k). The client (C) 10, in one embodiment, then encrypts (step 180) the second key (r) with the first key (k) to generate a fourth message ({r}k) 65. The client (C) 10 then sends (step 185) the fourth message ({r}k) 65 over the communication channel 15 to the server (S) 30.

The first computer (S) 30 next decrypts (step 190) this fourth message ({r}k) 65 using its first key (k) to obtain the second key (r). If the second key (r) received from the fourth message ({r}k) 65 is identical to the second key (r) which the server (S) 30 used to encrypt the first message ({k}r) 63, then the client (C) 10 is authenticated (step 195) to the server (S) 30. Thus the combination of multiple keys and multiple devices increases the amount of security in the authentication scheme.

In greater detail, when the user (U) logs onto the client (C) 10, he or she typically enters his or her username (U) and password (pw) (step 100). The client (C) 10 transmits

(step 105) the user's username (U) as a login message 20 to the server (S) 30 over the communication channel 15, which in one embodiment may be a secure confidential communication channel. Once this login message 20 is received by the server (S) 30, the server (S) 30 generates (step 110) the first key (k) and the second key (r), which in one embodiment are random numbers. The server (S) 30 encrypts (step 120) this first key (k) with the second key (r) and transmits (step 125) the first message 63 ({k}r) to the client (C) 10 over the communication channel 15. Although in this embodiment the first key and the second key are random numbers that the server (S) 30 generates, in another embodiment such first and second keys may have predefined values. The first key (k) and a second key (r) may take on any specific values that the server (S) 30 expects to receive back from the client (C) 10 upon authentication as described below.

In one embodiment, the server (S) 30 uses the user's username (U) from the login message 20 to look up a public key (u+) associated with the user (U) and to define a method to communicate with the verifier 50 associated with the user (U). In one embodiment the method includes selecting the communication channel 40, which, in one embodiment, may be the user's mobile phone number. The server (S) 30 then generates (step 130) a second message 35, which may be designated as (S,{U,{r}u+}s-). The server (S) 30 transmits (step

135) the second message 35 to the verifier 50 over the communication channel 40, which in one embodiment may be a secure confidential communication channel.

As indicated previously, in one embodiment this second message 35 includes an encrypted portion and a non-encrypted portion. In one embodiment the encrypted portion includes the second key (r) encrypted with the user's public key (u+). The encrypted portion also includes the user's username (U) and the second key encrypted with the user's public key (u+), both encrypted with a private key (s-) associated with the server (S) 30. As a result of the encryption, the encrypted portion may be designated ({U,{r}u+}s-). The non-encrypted portion of the second message 35 includes the server 30 designation (S). As a result, the second message 35 may be designated as (S,{U,{r}u+}s-).

The verifier 50 receives the second message 35 (S,{U,{r}u+}s-) over the communication channel 40 and uses the non-encrypted server 30 designation (S) to obtain the server 30's public key (s+) from the verifier 50's memory. Using this public key (s+), the verifier 50 decrypts the encrypted part ({U,{r}u+}s-) of the second message 35 to obtain the user's username (U) (step 140) and the second key encrypted with the user's public key ({r}u+). With this information about the user (U), the verifier 50 obtains the user's private key (u-) from its memory in order to access the second key (r), which was encrypted with

the user's public key (u+). In one embodiment, the verifier 50 can only access the user's private key (u-) encrypted with the user's password (w). The use of the separate user password (w) by the verifier 50 is to prevent the vital second key (r) from being reported to an unauthorized user. In one embodiment, the verifier 50 reports the user's username (U) on the mobile phone display and subsequently requests the matching user password (w). The user types in his or her password for the mobile phone and the phone decrypts ({u-}w) using the password (w) to obtain the user's private key (u-). With the user's private key (u-), the verifier 50 recovers (step 140) the second key (r) by decrypting ({r}u+), which was transmitted as part of the second message 35.

In another embodiment, the verifier 50 authenticates the server (S) 30 and thereby ensures the validity of the received second message 35 (as shown in phantom 142 in Fig 1). For this to occur, the server (S) 30 generates (step 115) a third key (n), which in one embodiment is another random number, and includes this in the non-encrypted portion and encrypted portion of a second message 35' (step 145). That is, the encrypted portion may be designated as ({n, U, {r}u+}s-). The second message 35' may then be designated as (S, n, {n,U,{r}u+}s-). The server (S) 30, as before, transmits (step 150) this second message 35'

to the verifier 50 over the communication channel 40. Again the verifier 50 decrypts (step 155) the encrypted portion ({n,U, {r}u+}s-) to obtain (U) and the third key (n).

The verifier 50 then checks (step 160) that the decrypted third key (n) is the same as the third key (n) sent in the non-encrypted portion of the message, thereby determining that the second message 35' was sent by the server (S) 30. Further, since the third key (n) in the non-encrypted portion should match the third key (n) in the encrypted portion of the second message 35'', if the second message 35' was intercepted and a new third key (n) was inserted in the non-encrypted portion of the second message 35' to form a second message 35'', the verifier 50 would detect the second message 35'' as unauthentic. Therefore, the third key (n) allows the verifier 50 to assure that both the encrypted portion ({n, U, {r}u+}s-) and the non-encrypted portion (S,n) of the second message 35' are current messages. The verifier 50 then decrypts (step 155) the remainder of the encrypted portion ({r}u+) using the private key (u-) of user (U), which the verifier 50 has in its memory, to obtain the second key (r).

Subsequent to the recovery of the second key (r), the verifier 50 transmits (step 170) the second key (r) to the client (C) 10 in a third message 60 (step 165). The third message 60 is sent (step 170) over a communication channel 55, which may be a secure confidential

communication channel. In one embodiment, the second key (r) recovered by the verifier 50 is produced on the mobile cellular phone display. The user (U) reads the second key (r) and types this second key (r) as message 60 into the client (C) 10. Thus in this embodiment the third message 60 is that displayed on the verifier, and the user (U) acts as the secure channel 55 carrying the third message 60 from the display of the verifier 50 to the client computer (C) 10. In another embodiment, the verifier 50 transmits the third message 60 over a direct electronic, radio, or optical communication channel 55 to the client (C) 10.

In one embodiment, the verifier 50 has a subscriber identification module (SIM) card, which is a smart card plugged into the mobile phone. The SIM allows the verifier 50 to store data in a tamperproof storage, access a private key associated with a particular user, decrypt the second message using the private key, and display a portion of the decrypted second message. In yet another embodiment, the verifier 50 has equivalent smart card properties.

In one embodiment, the client (C) 10 uses the desired second key (r) received in the third message 60 to recover (step 175) the first key (k) from the first message 63 ({k}r). The second key (r) and the user's login password (pw) are then encrypted (step 180) with the first key (k) and transmitted (step 185) to the server (S) 30 in a fourth message 65 ({r,

pw}k) over the communication channel 15. The server (S) 30 decrypts (step 190) the fourth message 65 and authenticates (step 195) the user and client (C) 10 to the server (S) 30 if the returned second key (r) agrees with the second key (r) used in the first message 63 ({k}r). The server (S) 30 also authenticates the user with the decrypted user login password (pw).

In another embodiment, the server (S) 30 starts a timeout period when the server (S) 30 transmits (step 135) the second message 35 to the verifier 50. Authentication of the client (C) 10 to the server (S) 30 will only occur if the fourth message 65 ({r,pw}k) is received within the timeout period and the second key (r) from the fourth message 65 is the same as the generated second key (r).

In another embodiment, the phone has full screen and keyboard functionality from an electronic, radio, or optical communication channel 40 to the server (S) 30. In yet another embodiment, the verifier 50 can be repeatedly challenged by the server (S) 30 via the client (C) 10 using the first and third communication channels 15 and 55, respectively, to encrypt a random number with the user's private key (u-) to guarantee proximity between the verifier 50 and the client (C) 10. If the verifier 50 is removed, the secure link between the verifier 50 and the server (S) 30 is broken. Furthermore, if the verifier 50 is later brought

back into the proximity of the client (C) 10, the secure link is automatically restored with the repeated challenges.

In one embodiment, the level of security obtained from the encryption technique used in the second message 35 increases as the number of devices, users, keys, and servers increase. Each encryption message can build from a previous encryption message to increase security. Some levels of security associated with different encryption messages are shown in the table below.

User Authentication	Multiple Users per Phone	Server Authentication	Multiple Servers per Phone	Message Number	Message
Secret key	No	None	No	1	{r}u
Public key	No	None	No	2	{r}u+
Public key	Yes	None	No	3	U{r}u+
Public key	Yes	Secret key	No	4	{U{r}u+}s
Public key	Yes	Private key	No	5	{U{r}u+}s-
Public key	Yes	Private key	Yes	6	S{U{r}u+}s-
Public key	Yes	Private key plus encrypted random number	Yes	7	S,n{n,U{r}u+}s-

A first message ({r}u) attains a level of authentication for one user per phone using a symmetric secret key (u) associated with the user and known by both the server (S) 30 and the verifier 50. A second message attains a greater level of security by encrypting the second key (r) with a public key (u+) associated with the user where the corresponding

private key (u-) is known only by the verifier 50. A third message (U{r}u+) allows for multiple users in a communication system by including in the message a username (U) associated with each user to determine what key to use for which user.

A single server can be authenticated with a fourth message that adds to the third message a symmetric secret key (s) associated with the single server. By replacing the symmetric secret key (s) with a private key (s-), a greater level of security is achieved because the private key (s-) has to be stored only on the server. A sixth message permits authentication of multiple servers included in a communication system with the addition of a server name (S) to the fifth message. The addition of this server name (S) allows one server to be authenticated from the multiple servers in the system. Further, a sixth key (n) is added to the sixth message to authenticate the message itself and to ensure that the message is current. Similarly, encryption messages can be built up further and further to achieve greater and greater levels of security.

In another embodiment, the verifier 50 does not store private keys but still enables the same level of mutual authentication between the server (S) 30 and the client (C) 10. Rather than storing private keys, the verifier 50 communicates with a trusted authentication server to certify messages. For example, after the verifier 50 receives the second message 35

(S,{U,{r}u+}s-), the verifier 50 still obtains the correct public key (s+) from the verifier 50's memory. Using this public key (s+), the verifier 50 decrypts the encrypted portion ({U,{r}u+}s-) of the second message 35 to obtain the user's username (U) and the second key encrypted with the user's public key ({r}u+).

To use the user's private key (u-), which is needed to access the second key (r), the verifier 50 sends the encrypted portion of the second message 35 to a trusted server (T). The trusted server (T) is a server that both the server (S) 30 and the verifier 50 trust and recognize as secure. In one embodiment the verifier 50 communicates with the trusted server (T) over a secure confidential communication channel. The trusted server (T) uses the username (U) to look up the user's private key (u-) and uses it to decrypt {r}u-. The trusted server (T) then transmits the second key (r) back to the verifier 50.

In yet another embodiment, the verifier 50 does not store public or private keys. As described above, the needed private keys are accessed by way of the trusted server (T). In a similar manner, the verifier 50 can obtain the needed public keys by way of the trusted server (T). Thus in this embodiment the verifier 50 can provide strong mutual authentication between the client (C) 10 and the server (S) 30 without memory, smart card properties, or direct access to keys.

It will be appreciated that the embodiments described above are merely examples of the invention and that other embodiments incorporating variations therein are considered to fall within the scope of the invention. In view of the foregoing, what I claim is: